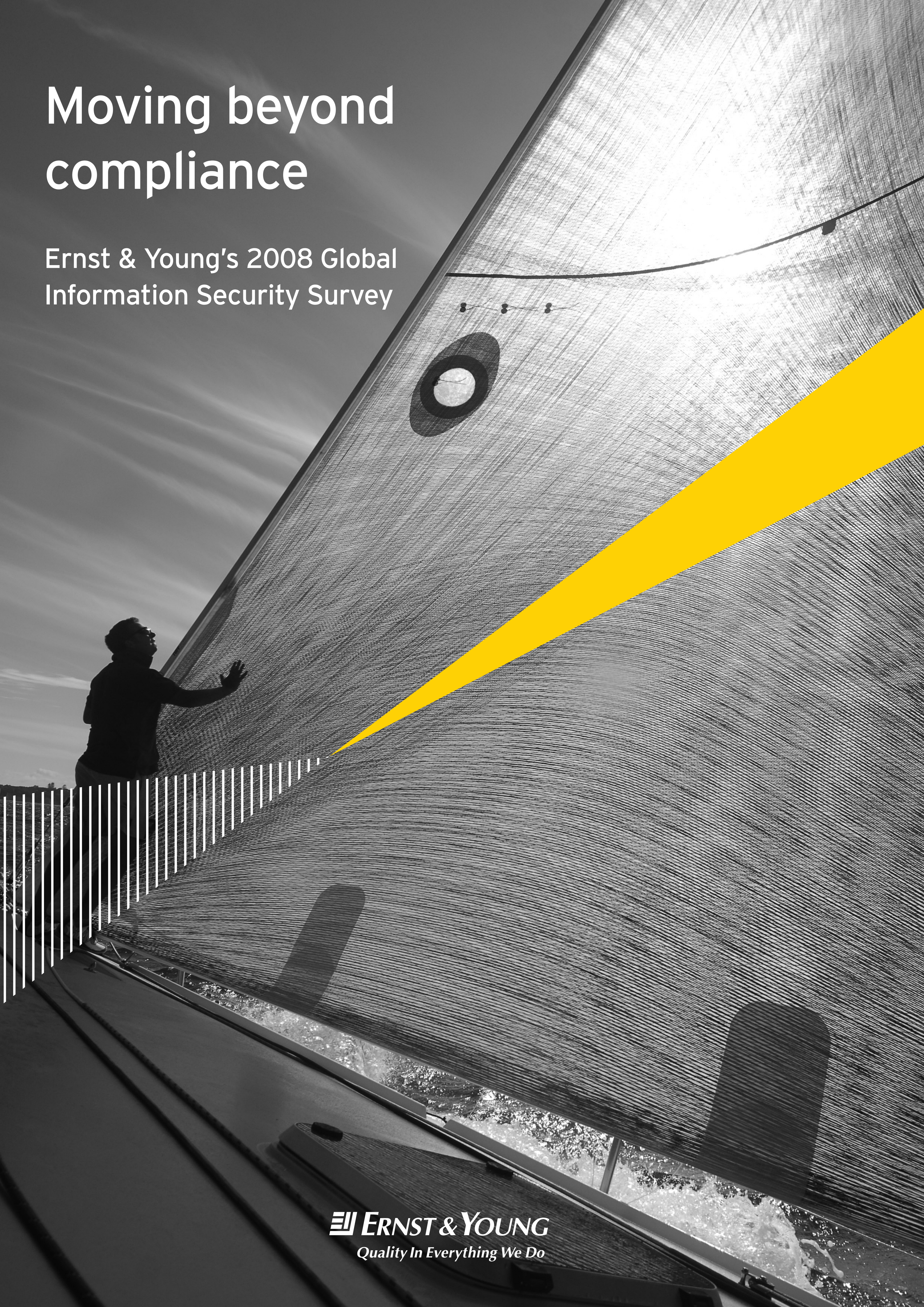
Moving beyond compliance

Ernst & Young's 2008 Global Information Security Survey



ERNST & YOUNG

Quality In Everything We Do

Contents

Paul van Kessel

Global Leader,
Technology and
Security Risk Services,
Ernst & Young

Foreword

The Ernst & Young global information security survey is one of the longest-running and most recognized annual surveys within the global information security arena.

I am proud that for more than a decade our survey has helped clients focus on the right information security priorities and risks, identify the strengths and weaknesses of their information security management systems and create an improvement agenda for the future.

Over the last several years, we have witnessed regulatory compliance drive improvements in information security. Although compliance has had a positive impact on most organizations, it is no longer the primary reason companies continue to make improvements in information security. This year, we see that protecting reputation and brand has become an important driver behind information security initiatives.

The survey results are encouraging in that many organizations are now moving beyond regulatory compliance requirements to continue to make improvements and protect their businesses from an increasing number of threats. However, our survey also reveals several important areas, like insider threats, privacy and third-party relationships, which many organizations still are not adequately addressing.

I would like to extend my warmest thanks to all of our 1,400 survey participants for taking the time to share their views on information security. My colleagues and I hope you find this survey report useful, informative and insightful. We welcome the opportunity to speak with you personally about your specific information security risks and how you can achieve real, sustainable performance improvements.

06.9
10.2

Introduction: moving beyond compliance

How do you convince your customers, trading partners and investors of your commitment to information security? How do you build confidence in your ability to protect their information? How do you protect your reputation and brand in an environment of escalating threats?

These are the challenges organizations face today and are now the primary drivers for information security. Over the last several years, regulatory compliance has helped improve information security, but meeting the minimal requirements for compliance does not address all of an organization's information security needs, nor provide any guarantees of protection. Organizations are realizing they must do more to effectively mitigate risks and achieve their business objectives.

Despite economic pressures, organizations are investing more in information security and adopting international information security standards at a much greater rate. These are clear indicators that many organizations are moving beyond compliance to strengthen their information security and making real, sustainable performance improvements.

In this *2008 Global Information Security Survey* we take a closer look at how organizations are specifically addressing their information security needs. We also identify and summarize potential opportunities for improvement and important trends that will continue to drive information security in the coming years.

Ten key findings

1. Protecting reputation and brand has become a significant driver for information security.
2. Despite economic pressures, organizations continue to invest in information security.
3. International information security standards are gaining greater acceptance and adoption.
4. Many organizations still struggle to achieve a strategic view of information security.
5. Privacy is now a priority, but actions are falling short.
6. People remain the weakest link for information security.
7. Growing third-party risks are not being addressed.
8. Business continuity is still bound to information technology.
9. Most organizations are unwilling to outsource key information security activities.
10. Few companies hedge information security risks with cyber insurance.

1. Protecting reputation and brand has become a significant driver for information security.

Damage to reputation and brand was cited as the most significant consequence of an information security incident by 85% of survey respondents. This finding, in combination with the concern for maintaining stakeholder confidence (77%), protection from the loss of revenues (72%) and the loss of customers (71%) are clear indicators for why information security remains a focus for most organizations.

The survey results reflect the fact that stakeholder confidence and a positive brand can take years to build, but can be severely damaged by a single incident. High-profile information security incidents reported in the media continue to be a reminder of how costly an information security failure can be and how vulnerable a company's reputation and brand are. According to Factiva, a Dow Jones company, media coverage of companies that suffered an information security breach accounted for more than half the stories written about those companies.

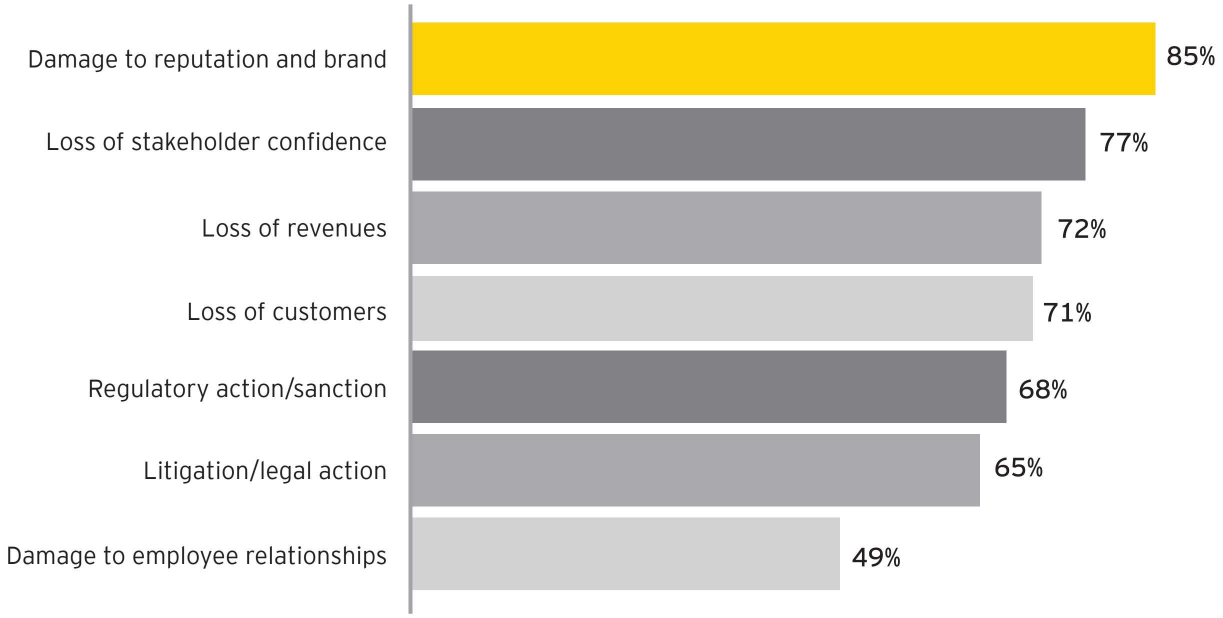
Since 2005, regulatory compliance has been the leading driver for information security. It has been an important catalyst for raising awareness and driving real improvements. Although cited by 68% of respondents as a driver for information security, compliance alone is not enough to ensure improvements continue to be made.

At Ernst & Young, we believe the need to protect reputation and brand has moved many companies beyond the requirements of regulatory compliance to strive to achieve a more integrated information security function. Companies need to build sustainable compliance programs while taking a more strategic and comprehensive view of information security.

The need to protect reputation and brand has moved many companies beyond the requirements of regulatory compliance.

Consequences of information security incidents

What is the level of significance for the following consequences if your organization's information is lost, compromised or unavailable?



Percentages based on responses of "significant" or "very significant."
Multiple responses permitted.

2. Despite economic pressures, organizations continue to invest in information security.

Several of the world's largest economies are experiencing a period of slowed economic growth, straining the performance of the global economy. During such times, many organizations become more conservative, tighten their budgets and look for alternate ways to reduce costs.

Historically, the IT function is one of the first to feel the pressure to reduce expenditures, and traditionally, information security has been closely linked with IT. Our survey confirms the link between IT and information security is still very strong (71% of respondents meet monthly with IT), but the pressure to reduce costs does not appear to be carrying over to the information security function. In fact, only 5% of respondents indicate they will be reducing annual expenditures for information security and 50% plan to increase their investment in information security as a percentage of total expenditures. In addition, only 33% of respondents cite adequate budget as a challenge to delivering their information security initiatives.

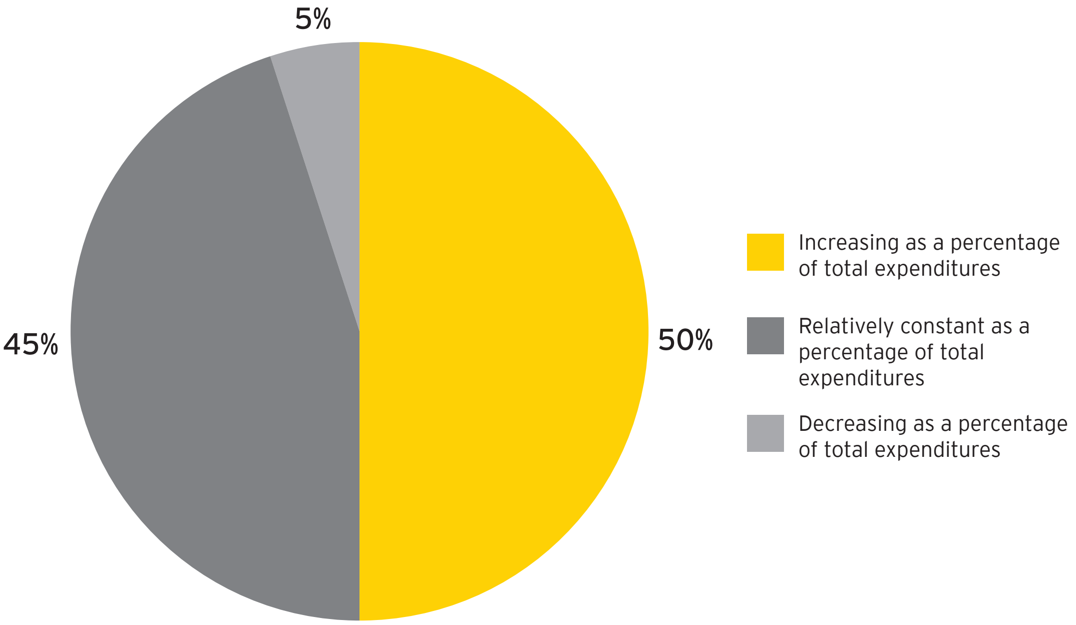
At Ernst & Young, we believe that organizations are continuing to invest in information security for two very good reasons: first, reducing information security expenditures would likely have a negative impact on the perceptions of key stakeholders (e.g., customers, trading partners and investors), and second, the threats, vulnerabilities and frequency of attacks do not diminish during an economic downturn — there is evidence to suggest they may actually increase.

Although investments in information security are not being reduced, organizations must determine whether these investments are being made in the right places. Only 20% of respondents have a documented strategy for information security and less than half perform formal risk analyses to direct information security activities. To help ensure they are getting the most benefit from their information security investments, organizations should establish a clear information security strategy and an integrated risk management approach.

Only 5% of survey respondents indicate they will be reducing annual expenditures for information security.

Investment in information security

Which of the following statements best describes your organization's annual investment in information security?



3. International information security standards are gaining greater acceptance and adoption.

More companies are using internationally recognized standards for information security. From 2007 to 2008, we noted an 8 percentage point increase in the number of survey respondents stating they incorporate information security standards (70%). When comparing the results from 2007 to 2008 for the use of specific information security standards, we find ISO/IEC 27001:2005 increased by 15 percentage points, ISO/IEC 27002:2005 increased by 9 percentage points and Information Security Forum's (ISF) *The Standard of Good Practice for Information Security* increased by 7 percentage points.

The survey results are not surprising, given the potential benefits of using international information security standards, including improved relationships with customers and trading partners, credibility with internal stakeholders and greater consistency across an organization.

The adoption of a recognized standard demonstrates and communicates that the company takes information security seriously. Stakeholder confidence is improved by knowing the company has taken an independently verifiable approach to information security risk management.

At Ernst & Young, we believe the use of international information security standards will continue to increase and that early adopters can potentially gain a competitive advantage. Just as quality management standards (e.g., ISO 9000) have become a requirement for doing business in certain industries, internationally recognized standards for information security will continue to gain acceptance and eventually become a necessity for many companies. This is primarily due to the fact that standards and certifications provide a level of confidence for customers and partners that is difficult to achieve by any other means.

Standards defined

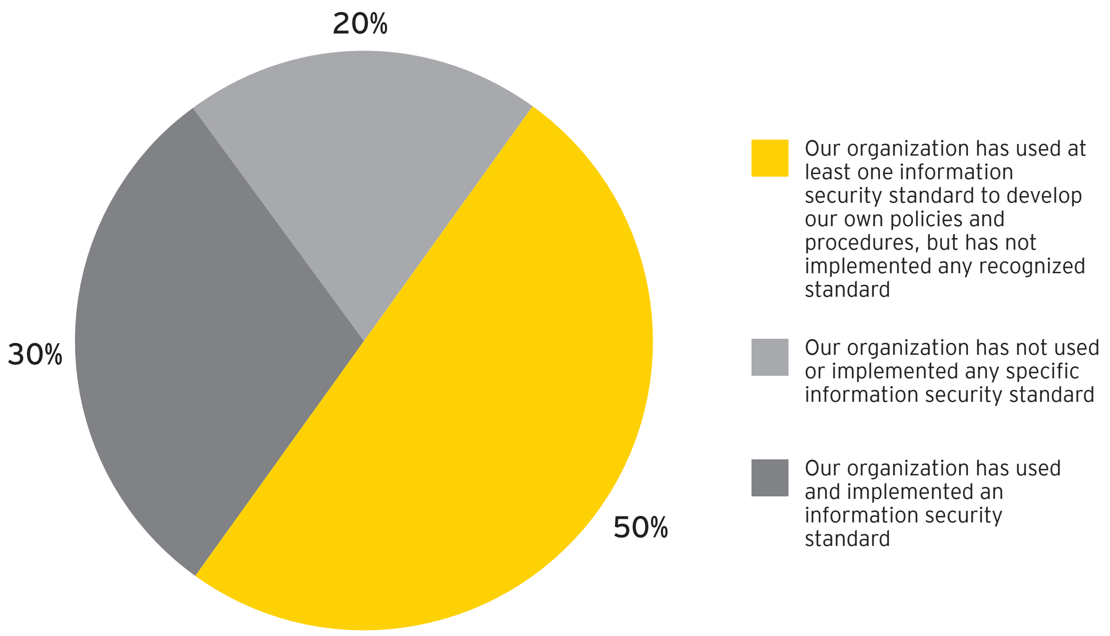
ISO/IEC 27001:2005 — This standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS).

ISO/IEC 27002:2005 — This standard outlines the potential controls and control mechanisms which may be implemented based on the guidance provided within ISO/IEC 27001:2005. It established guidelines and general principles for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security management within an organization.

Information Security Forum's (ISF) *The Standard of Good Practice for Information Security* — This standard addresses information security from a business perspective, providing a practical basis for assessing an organization's information security arrangements.

Information security standards

Which of the following statements best describes your organization's use of information security standards (e.g., ISO/IEC 27002:2005)?



4. Many organizations still struggle to achieve a strategic view of information security.

Information security has continued to improve, driven first by technical threats, then by regulatory compliance efforts and now by the need to protect reputation and brand. However, our survey suggests organizations still struggle to achieve a strategic view of information security that is aligned with the business.

We must commend the 18% of the organizations that indicated that information security was an integrated part of the organization's business strategy. The 20% of respondents that indicated they had developed a specific information security strategy have taken a critical first step, but to be fully effective, it still needs to reflect the organization's business priorities. A respectable 33% indicated that their information security strategy was integrated as part of the organization's IT strategy. Presupposing that the IT strategy is tied into the business, this is an excellent result. Most troubling is that 29% of the organizations surveyed had no information security strategy at all.

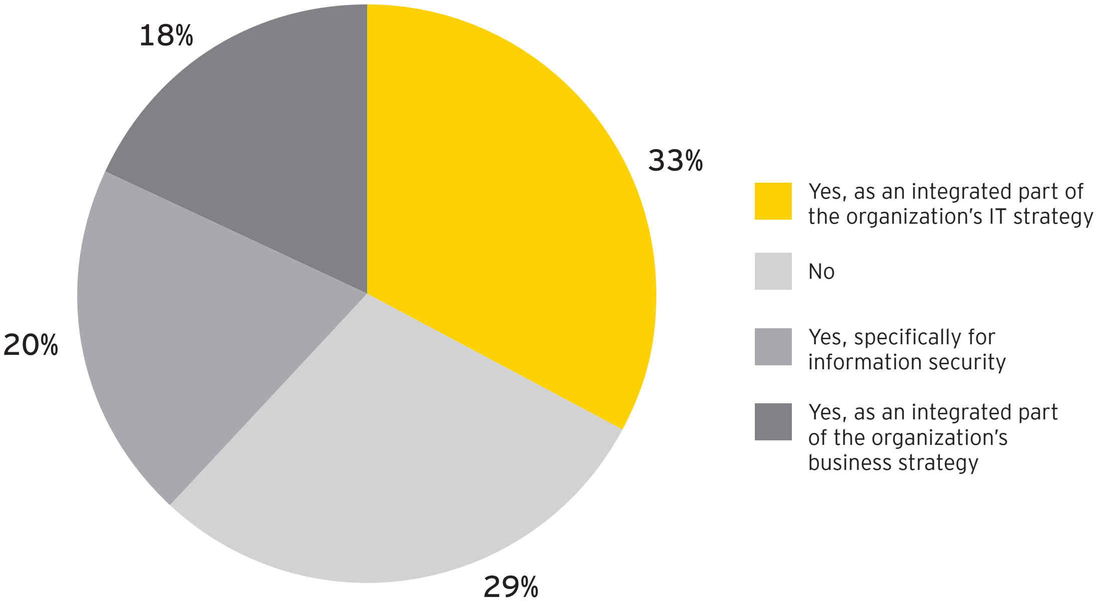
Developing an information security strategy that integrates with the business strategy is critical to the success of information security and to fully addressing the risks to the organization. Organizations are beginning to understand how important information security is in not only supporting regulatory compliance, but also in protecting their reputation and brand.

At Ernst & Young, we believe the challenge for many organizations is not just how to make information security work better with the business, but to fully integrate information security and make it a part of the business. This is a two-part process. First, more organizations must be willing to bring information security into those strategic discussions as a valuable partner. Second, those responsible for information security must reach out and take a more business-centric view, getting involved in discussions about the changing organizational culture, establishing reliable processes and developing training and awareness programs for employees. Leading organizations have found that once these two objectives have been achieved, information security becomes more strategic.

Organizations must be willing to bring information security into strategic discussions as a valuable partner.

Information security strategy

Does your organization have a documented information security strategy for the next one to three years?



5. Privacy is now a priority, but actions are falling short.

Privacy continues to be an important driver for information security and a priority for many organizations. The increasing pool of regulations that require "reasonable" protection of personal information are enough to compel action. But it is the consequences of privacy-related information security incidents that accelerate the need for that action. As stated previously, our survey respondents cite damage to reputation and brand (85%) and loss of stakeholder confidence (77%) among the highest areas of concern. This is not surprising, given that the costs and damages related to these privacy risks often outweigh the risk of regulatory noncompliance.

The survey results exposed a disconnect between what some organizations reported for information security in general, and what they reported for privacy and safeguarding personal information in particular. For example, 86% of respondents indicated that they have at least a partial inventory and classification of information. However, only 31% have produced an inventory of information assets covered by privacy requirements. Similarly, about 96% indicated that they conducted information security assessments, but only 27% indicated that they conducted assessments of personal information — or a privacy assessment.

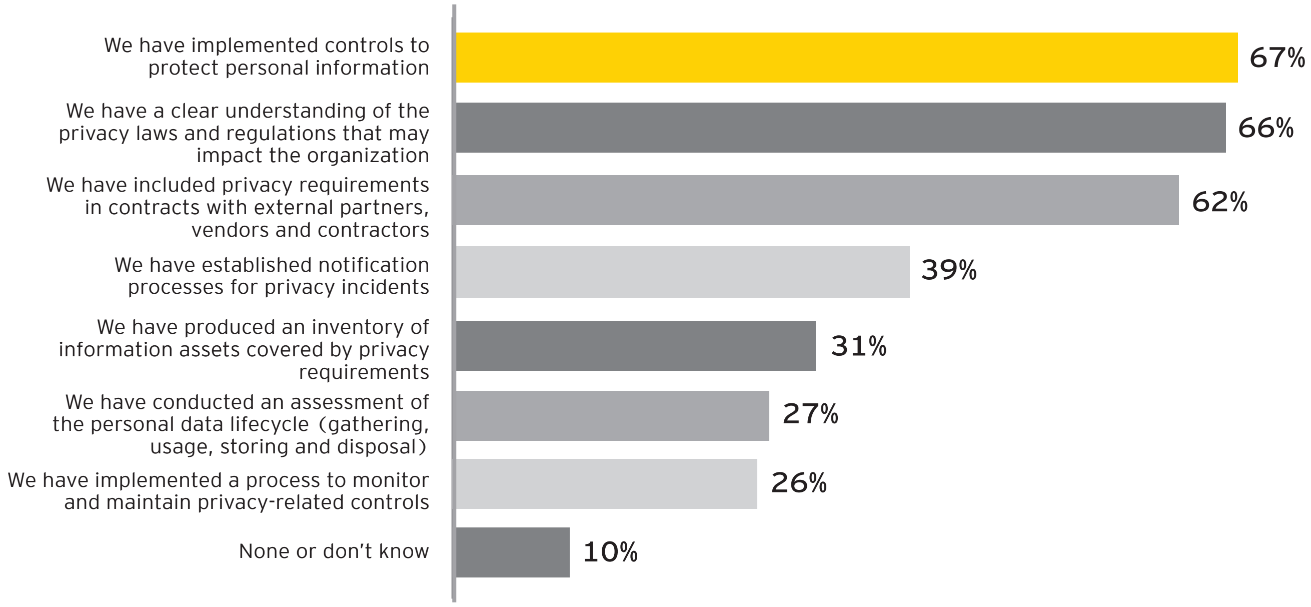
This is likely due to the fact that information security has been largely driven by the internal controls requirements for financial processes. More recently, organizations have begun to address the other high-priority compliance and risk drivers related to the use of information technology, such as privacy.

At Ernst & Young, we believe that organizations must take a more comprehensive view of their IT risks and compliance obligations, including those for privacy and protection. And address these risks and obligations to a more rigorous level than they do for other information.

Only 31% of survey respondents have produced an inventory of their organization's information assets covered by privacy requirements.

Privacy

Which of the following statements can be made by your organization regarding privacy?



Multiple responses permitted.

6. People remain the weakest link for information security.

Investments in technology are of little value unless people are trained on what to do and how to do it. This has been recently reinforced by several high-profile information security breaches where it was eventually determined to be a human failure that brought about the incident and not a technical vulnerability.

So much emphasis is often placed on technology that the "people" component of information security is frequently overlooked. This year's survey results confirm this is still an unaddressed issue for many companies. Organizational awareness was cited by 50% of respondents to be the most significant challenge to delivering successful information security initiatives – more significant than the availability of resources (48%), adequate budget (33%) and addressing new threats and vulnerabilities (33%).

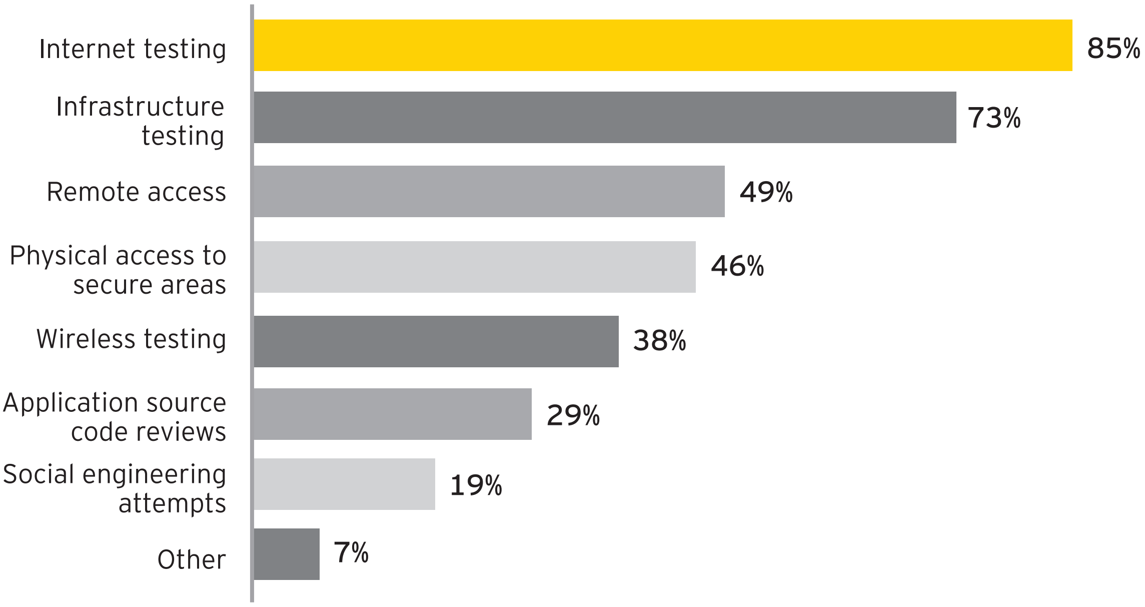
Hackers have long known the easiest way to circumvent an information security system is to exploit the people. Simple techniques – such as impersonating IT or company personnel – can be used to gain access to information from unsuspecting employees. A large percentage of respondents (85%) confirmed that they regularly perform internet testing, but only 19% of respondents conduct social engineering attempts to test their employees.

At Ernst & Young, we believe that technology plays a pivotal role in information security, but there must also be a focus on training and awareness programs for information security to operate effectively. Organizations must view their people to be as critical as any other information security component – so they can help prevent and properly respond to information security incidents in an effective and timely manner.

Organizational awareness was cited by 50% of respondents to be the most significant challenge to delivering successful information security initiatives.

Information security testing

Which of the following types of attack and penetration testing does your organization regularly perform?



Multiple responses permitted.

7. Growing third-party risks are not being addressed.

Now more than ever, companies are sharing data and sensitive information with vendors and contractors. In our connected economy, the flow of information is a vital part of doing business and will continue to increase with trends in globalization, fragmentation and outsourcing.

Companies are now realizing that sharing data with a third party rarely transfers the risk or responsibility for protecting the information. Organizations must take steps to safeguard information even when it has left the protection of their own information systems. This includes ensuring that the third-party organization conforms to an equivalent set of information security policies and controls.

There is evidence from our survey that many organizations are struggling to address third-party risk. Only 45% of respondents include specific requirements for information security in all of their contracts with partners, vendors and contractors. In addition, 29% of respondents indicated that they do not perform any type of review, audit or assessment of the third parties with whom they exchange information.

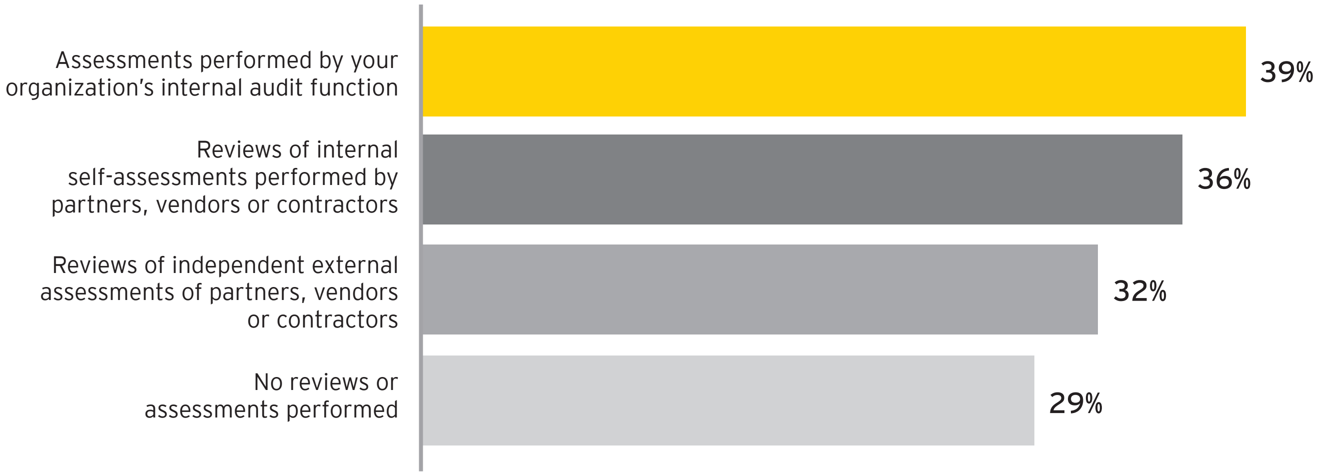
Companies that are successfully dealing with this issue understand that their own information security and privacy policies must be "portable." The policies and controls must travel with the data and the responsibility for protecting information must also be shared by all third-party organizations.

At Ernst & Young, we believe one of the most effective ways to build confidence in your business partners' ability to protect your organization's information is through specific contractual requirements and consistent controls. To validate compliance with these requirements, leading organizations encourage the adoption of international information security standards and conduct periodic third-party assessments.

Organizations must take steps to safeguard information even when it has left the protection of their own information systems.

Third-party risk

How do you ensure that your external partners, vendors and contractors are protecting your organization's information?



Multiple responses permitted.

8. Business continuity is still bound to information technology.

For many organizations, the primary responsibility for business continuity management (BCM) remains with IT. Of this year's survey respondents, 41% indicated the responsibility for BCM was with their IT function, 20% placed it under risk management and 11% have given the responsibility to information security. The challenge with this alignment is that IT traditionally has focused on disaster recovery rather than full business continuity. Our survey supports this premise as 51% of respondents perform disaster recovery simulation testing, but only 34% perform business continuity simulation testing. In the event of a business disruption, an organization may be able to restore networks and information systems, but unable to provide the support needed for the people or the critical business processes.

An area of pressing need from a business continuity perspective is crisis management. Only 24% of the respondents ran crisis management testing that involved business and executive management. This lack of testing involving business leadership could mean that when a business interruption occurs, the company leadership is ill prepared to help manage the crisis. This disconnect is troubling when the protection of reputation and brand appears to be of critical importance.

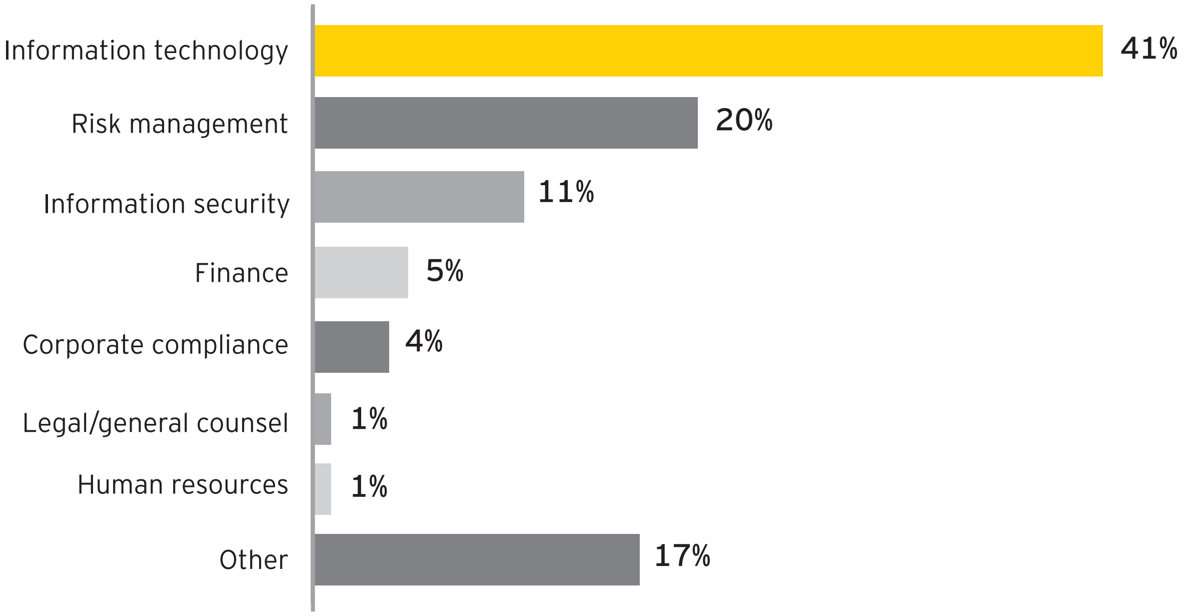
On a positive note, 77% of organizations have identified their critical business processes and a further 72% have documented procedures for managing incidents, disasters and crises. Organizations are taking steps in recognizing areas of risk and attempting to mitigate that risk through the use of defined procedures.

At Ernst & Young, we believe organizations need to look at BCM as a critical risk management function and consider moving the business continuity function away from IT to risk management or another business-level management function. BCM needs to be placed where their lines of communication to executive leadership are clear. In addition, all levels of the organization, especially executive leadership, should be involved in the testing process. So that if a business interruption does occur, it is not the first time the BCM plans are used.

For 41% of our survey respondents, the responsibility for business continuity has been assigned to the IT function.

Business continuity

Which functional area of your organization has primary responsibility for BCM?



Multiple responses permitted.

9. Most organizations are unwilling to outsource key information security activities.

Outsourcing is a strategy that continues to gain momentum — fueled by economic pressures and resource constraints. In Ernst & Young's *2008 European outsourcing survey*, 23% of respondents indicated an intention to outsource, or enlarge the scale of their outsourcing, over the next two years. One of the most frequently outsourced activities is the IT function with 37% of respondents planning to outsource within the next two years.

Despite the trend to outsource, most organizations are unwilling to externalize information security activities. A small percentage of our survey respondents indicated they outsource incident response activities (15%) and forensic investigations (19%). In discussing outsourcing with key clients, it became apparent that even when they do outsource information security activities, they only outsource a small portion of the work — keeping the majority of the work in-house.

It is clear that organizations are reluctant to give up control of activities related to actual information security incidents or breaches. This is consistent with our other survey findings. Most organizations believe that protecting the reputation and brand is too important to transfer to an outside provider.

There were several exceptions to this unwillingness to outsource information security activities and these included information security assessments (50%) and attack and penetration testing (59%). These two activities are also expected to increase significantly with 15% and 18% respectively planning to outsource this work.

At Ernst & Young, we believe each company faces a unique situation with many competing factors when considering outsourcing decisions. To be successful, companies must continually assess which activities to outsource and which to retain in-house in order to achieve a balance that provides the most benefits to the company and its stakeholders.

Organizations are reluctant to give up control of activities related to actual information security incidents.

Outsourcing

Which of the following security-specific activities have been outsourced or considered for outsourcing?

	No plans to outsource	Currently outsourced (full or partial)	Under evaluation/ planned for outsourcing
Security assessments/audits	35%	50%	15%
Attack and penetration testing	23%	59%	18%
Application testing	56%	30%	14%
Security training and awareness	62%	21%	17%
Vulnerability/patch management	67%	24%	9%
Disaster recovery/business continuity management	65%	22%	13%
eDiscovery, forensics/fraud support	66%	19%	15%
Incident response	77%	15%	8%
Help desk (password reset/ access issues)	66%	27%	7%

10. Few companies hedge information security risks with cyber insurance.

About six years ago, insurance companies started offering cyber insurance policies to protect companies from the risks associated with hacker attacks, online privacy violations and other information security incidents. These policies provide another layer of risk mitigation for potentially significant losses. Although most organizations would gladly turn a variable risk into a fixed cost, cyber insurance has not yet gained wide acceptance or adoption. In fact, only 13% of respondents currently have insurance coverage for the losses resulting from an information security incident and 5% of respondents cite an intention to purchase a cyber insurance policy within the next year. Our survey also revealed that 37% of respondents did not know whether they had this type of insurance coverage.

Insurance providers have struggled to determine appropriate premium rates since cyber risk is difficult to quantify and without a large amount of supporting actuarial data. Many companies have not purchased cyber insurance due to the cost and substantial number of exclusions typically written into these types of policies. However, as insurance companies get better at evaluating the threats and risks to an organization, the costs should decline and the number of exclusions should diminish. In addition, the adoption of international information security standards, will help companies demonstrate their information security capabilities and avoid additional third-party information security audits often mandated by the insurance providers.

At Ernst & Young, we recognize that insurance decisions may not fall under the domain of the information security function, but we believe it is important that those responsible for information security are part of the discussion and have an understanding of what coverage they do have.

For most companies, insurance can be an important risk mitigation tool and, if used appropriately, it can effectively supplement information security measures to provide a more comprehensive risk management solution.

Only 13% of survey respondents currently have insurance coverage for the losses resulting from an information security incident.

Insurance

In the event of a cyber attack, does your organization presently have, or is it contemplating the purchase of an insurance policy to cover the following?

	Presently have	Plan to purchase within 12 months	Do not have plans	Don't know
Costs of responding to the incident	12%	4%	49%	35%
Losses resulting from lost profits and business income during the incident	13%	5%	45%	37%
Coverage for both insider and outsider attacks	12%	5%	48%	35%
Costs of civil litigation including defense, settlements and judgments	12%	3%	44%	41%
Costs of regulatory investigations arising out of theft of personal identifiable information	9%	4%	46%	41%
Costs of notification to affect persons	7%	4%	49%	40%
Crisis management expenses	11%	4%	47%	38%
Damage to data and reconstruction costs	17%	6%	41%	36%

2009 and beyond

2009 and beyond

This year's survey confirms a shift from regulatory compliance-driven information security to business improvement and stakeholder-driven information security. What this means is that information security continues to evolve as it adapts to the almost overburdening task of making information available, but also secure.

At Ernst & Young, we believe information security can no longer be an afterthought, it must be fully integrated into the business. It is no longer sufficient to just have the correct controls in place. You must be able to prove that the controls work consistently and that information is available and secure regardless of when and where it's used. Moving from compliance-driven information security requirements to a focus on the needs of the stakeholders presents new and demanding challenges for organizations and their information security professionals.

Because of this shift in focus, it is imperative that organizations continue to make investments in information security, even with the global economies experiencing a downturn. These investments are not only necessary to maintain the current levels of protection, but needed to help ensure that additional safeguards and improvements are achieved.

Now, more than ever, is the time to make information security strategic to the organization. Moving beyond compliance means moving beyond the fire-fighting, tactical approach of addressing threats and vulnerabilities.

This, of course, does not come without significant challenges. Creating an effective framework, based on the adoption of internationally accepted information security standards, is a critical step toward truly integrating information security into the business.

Finally, it's no longer safe to assume that threats always come from "outside" the organization. A comprehensive and strategic view of information security must account for all areas of risk, including insiders and business partners.

By leveraging the information in this survey and taking action on the opportunities for improvement presented, organizations can continue to move beyond compliance and achieve more effective and integrated information security.

At Ernst & Young, we believe organizations should:

1. Establish a clear information security strategy and an integrated risk management approach

2. Enhance the current compliance programs to be more sustainable while taking a more strategic and comprehensive view of information security

3. Bring information security into strategic business discussions as a valuable partner

4. Adopt internationally recognized standards and frameworks for information security

5. Address the risks associated with privacy and personal information at a more rigorous level

6. Involve executive leadership in business continuity management with clear lines of communication

7. Focus on information security training and awareness programs to operate more effectively

8. Establish specific information security requirements and controls for third-party contracts

9. Continually assess outsourcing options to achieve a balance that provides the most benefits to the company and its stakeholders

10. Leverage cyber insurance to effectively supplement information security measures

Survey approach

Survey approach

Ernst & Young's *Global Information Security Survey*, now in its 11th year, gauges the current state of information security and the major factors shaping its future.

This year's survey was conducted from 6 June 2008 to 1 August 2008. Nearly 1,400 organizations in more than 50 countries and across all major industries participated.

The questionnaire used in the 2008 survey was designed to gather information on the following key aspects of information security:

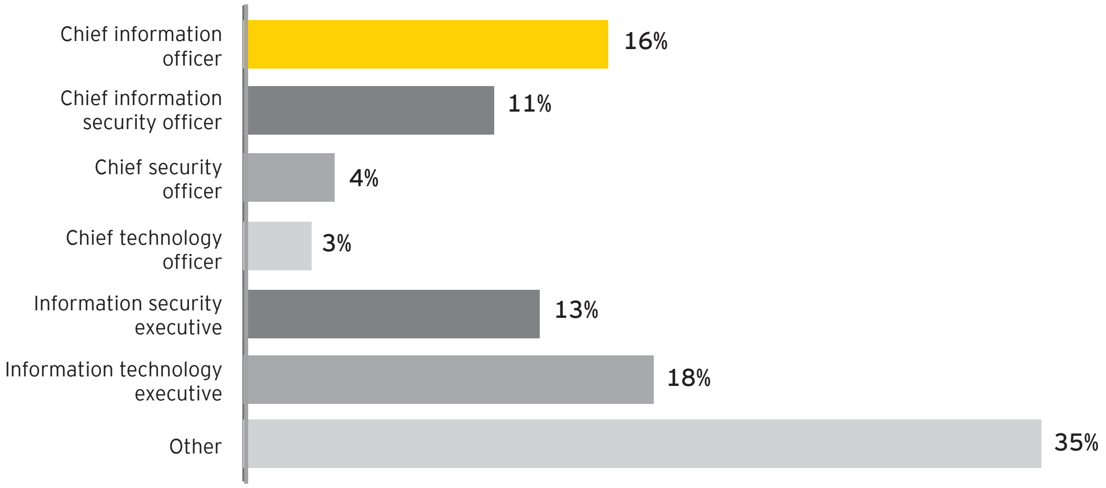
- Governance and measurement
- Organization
- Drivers
- Standards
- Activities

The questionnaire was distributed internationally to designated Ernst & Young professionals in each country practice, along with instructions for consistent administration of the survey process.

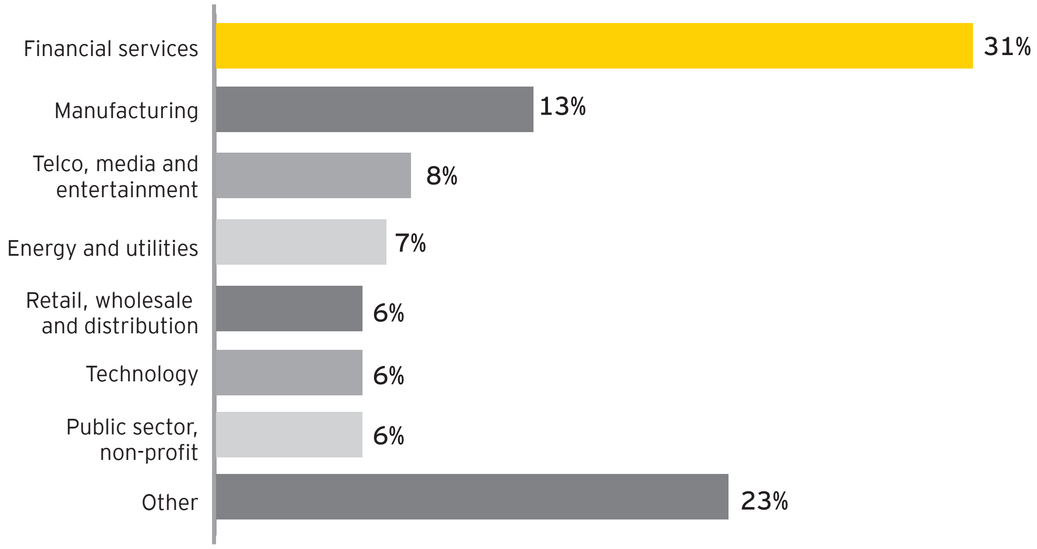
Most of the survey responses were collected during face-to-face interviews with individuals responsible for information security at the participating organizations. When this was not possible, the questionnaire was administered electronically.

If you wish to participate in Ernst & Young's *2009 Global Information Security Survey* you can do so by contacting your local Ernst & Young office or visiting **www.ey.com/giss** and completing a brief request form.

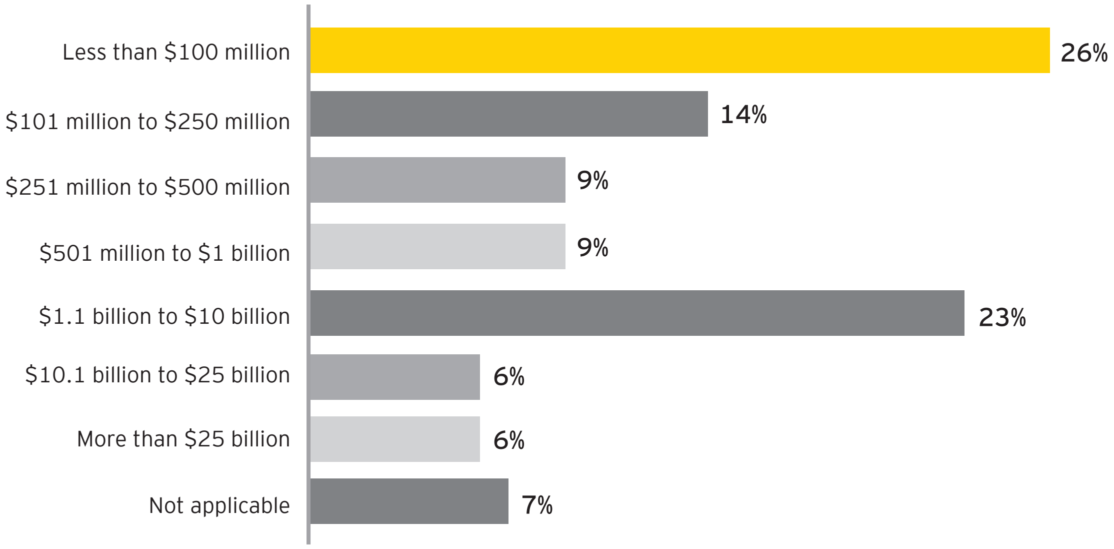
Survey participants by job title



Survey participants by major industry group



Survey participants by annual revenue (US$)



Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 135,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

About Ernst & Young's Technology Risk and Security Services
Information technology is one of the key enablers for modern organizations to compete. It gives the opportunity to get closer, more focused and faster in responding to customers, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective information technology risk management helps you to improve the competitive advantage of your information technology operations, to make these operations more cost efficient and to manage down the risks related to running your systems. Our 6,000 information technology risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your information technology risk or to deal with a specific risk and security issue. And because we understand that, to achieve your potential, you need a tailored service as much as consistent methodologies, we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

© 2008 EYGM Limited.
All Rights Reserved.

EYG no. AU0162

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

www.ey.com/security